EU-Außenhandel und Datenschutz: wie lässt sich beides besser vereinbaren?

Bendiek, Annegret; Schmieg, Evita

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Stiftung Wissenschaft und Politik (SWP)

SWP-Aktuell

Stiftung
Wissenschaft und
Politik

Deutsches Institut
für Internationale
Politik und Sicherheit

EU-Außenhandel und Datenschutz

Wie lässt sich beides besser vereinbaren?

Annegret Bendiek / Evita Schmieg

Der Handel mit digitaler Technologie und digitalen Dienstleistungen hat sich zu einem überaus wichtigen Element der internationalen Wirtschaftsbeziehungen entwickelt. Ein großer Teil dieses Handels ist mit dem Transfer von Daten verbunden, die zum Teil personenbezogen sind. Viele der inzwischen im Umfeld des Internets entstandenen Produkte und Dienstleistungen weisen neue datenschutzrelevante Eigenschaften auf. Insofern besteht heute erheblicher Regelungsbedarf, der eine verstärkte Kooperation von Fachleuten für Handelsrecht, Datenschutz und Informations- und Kommunikationstechnologie (IKT) verlangt. Dies gilt vor allem für die derzeitigen Verhandlungen über die Transatlantische Handels- und Investitionspartnerschaft (TTIP) und für das neue Abkommen zum transatlantischen Datentransfer (EU-US Privacy Shield).

Die Staaten und das internationale Handelssystem hinken mit ihrer Regelsetzung den technischen Entwicklungen im digitalen Sektor hinterher. Der Europäische Gerichtshof (EuGH) und die EU-Kommission haben in jüngster Zeit rote Linien für multinational agierende Internet-Unternehmen vorgezeichnet, die aber noch in konkrete Gesetze gefasst werden müssen. Als Grundlage für transatlantische Regelungen wie etwa EU-US-Privacy Shield gilt die Datenschutz-Grundverordnung (DS-GVO) der Europäischen Union (EU). Gleichzeitig verhandelt die EU mit 23 Staaten über ein internationales Dienstleistungsabkommen (Trade in Services Agreement, TiSA) sowie mit den USA über die Schaffung des weltweit größten Wirtschaftsraums, der mit TTIP entstehen soll. Vor allem die deutsche Zivilgesellschaft bewertet die TTIP-Verhandlungen vor dem Hintergrund der NSA-Affäre kritisch. Dabei ist der Datenschutz kein Gegenstand der TTIP-Verhandlungen. Im Juli 2000 war die Übermittlung von Daten aus einem Land der EU an die USA durch die sogenannte Safe-Harbor-Entscheidung der Kommission geregelt worden. Nach dem Safe-Harbor-Urteil des EuGH vom Oktober 2015 ist eine auf diese Entscheidung gestützte Datenübermittlung nicht mehr zulässig. Anfang Februar 2016 haben sich EU und USA auf das Nachfolgeabkommen EU-US Privacy Shield geeinigt.

Bedeutung des Handels mit Daten

Vor allem durch die Nutzung des Internets hat die Übermittlung von Daten und der

Dr. Annegret Bendiek und Dr. Evita Schmieg sind Wissenschaftlerinnen in der SWP-Forschungsgruppe EU/Europa

Handel mit Dienstleistungen, die den Datenschutz betreffen, erheblich an Bedeutung gewonnen:

- als Nebenprodukt der Nutzung digitaler Dienstleistungen (der Transfer z.B. von Daten bei der Nutzung digitaler Versicherungsdienstleistungen);
- beim Managen globaler Wertschöpfungsketten durch internationale Unternehmen mit dezentralisierter Produktion;
- bei der Kommunikation;
- beim Abschöpfen des Wissens von Nutzerinnen und Nutzern zur Weiterentwicklung von Produkten;
- bei der Zusammenarbeit von Wissenschaftlerinnen und Wissenschaftlern im Rahmen von Forschung und Entwicklung, individuell und unternehmensintern;
- als Handel mit Daten (z.B. Consultingleistungen, Software, Bezahlung geistiger Eigentumsrechte, Verkauf von Statistiken über die Nutzung von Internetdiensten).

Daten werden heute auch von Maschinen und Anlagen generiert (z.B. von Triebwerken, Aufzügen, Autos). Ein Export solcher Produkte zieht ebenfalls Transaktionen im Dienstleistungssektor nach sich. Die Daten können beispielsweise Grundlage sein für Wartungs- und Reparaturarbeiten. Die Erbringung solcher »after-sales-services« hängt davon ab, welche Regelungen für die Rechte an diesen Daten getroffen wurden. Verbleiben sie beim Exporteur des Produkts, kann er selbst die Wartungsarbeiten als Dienstleistungsexport durchführen. Waren erzeugen ihrerseits Daten und sind digital vernetzt – wie etwa Smartphones oder -watches – und bilden das sogenannte »internet of things«. Die Nutzung und Auswertung dieser Daten ist auf einen freien internationalen Datenfluss angewiesen. Die These, die Konsumenten würden der Verarbeitung von Daten grundsätzlich zustimmen, ist problematisch. Vielfach verfügen sie nicht über die nötigen IT-Kenntnisse, um Datenschutzmechanismen anzuwenden. In der Abwägung zwischen Datenschutzinteresse und Interesse an der Nutzung angebotener Dienste überwiegt dann letzteres. Gerade viele deutsche Verbraucherinnen und Verbraucher haben aber ein großes Interesse daran, dass ihre Daten besser geschützt werden. Datenschutzbedenken sind indes von Gesellschaft zu Gesellschaft unterschiedlich gelagert.

Digital verfügbare Dienstleistungen – etwa Beratung über das Internet – gewinnen zunehmend an Bedeutung. An den transatlantischen Dienstleistungsexporten haben sie heute bereits einen Anteil von mehr als 50% (USA 72%, EU 63%). Sie liefern zugleich wichtige Inputs für die Produktion von Exportgütern. Große Wirtschaftsbereiche sind daher am Export dieser Produkte interessiert, aber auch an einem verbesserten Zugang zu Importen, der dazu beiträgt, Kosten zu senken und die Wettbewerbsfähigkeit zu steigern. Laut United States International Trade Commission (USITC) reduziert das Internet die Handelskosten um durchschnittlich 26%. Vor allem in Entwicklungsländern dürfte der Markt für digitale Dienstleistungen rasant wachsen. Ein großer Teil der Welt wird das Internet mit mobilen Geräten erschließen, davon werden 2018 54% »smart« sein (21% waren es im Jahr 2013). Eine wachsende Mittelklasse, die sich etwa in Asien bis 2020 verdoppeln wird, verweist auf das große Potential für den Onlinehandel.

Internationale Handelsabkommen

Der Dienstleistungshandel wird seit 1995 im Rahmen der Welthandelsorganisation (World Trade Organization, WTO) durch das Allgemeine Abkommen über den Handel mit Dienstleistungen (General Agreement on Trade in Services, GATS) geregelt. Ein gesondertes Abkommen gewährt Zollfreiheit für bestimmte informationstechnologische Produkte – das Informationstechnologie-Abkommen. Das GATS schafft einerseits allgemeine Verpflichtungen: Nach dem Meistbegünstigungsprinzip müssen alle Handelspartner gleich behandelt werden. Zudem gelten Transparenzvorschriften. Andererseits wird eine Liberalisierung

des Handels mit Dienstleistungen erreicht, indem spezifische Verpflichtungen für die Gewährung des Marktzugangs und für Inländerbehandlung gelten (national treatment), nach der ausländische Dienstleistungsanbieter inländischen gleichgestellt werden. Die Liberalisierungsverpflichtungen der einzelnen WTO-Mitgliedstaaten sind in den sogenannten Liberalisierungslisten (schedules) aufgeführt.

Das GATS unterscheidet vier Möglichkeiten (sogenannte Erbringungsarten, engl. »modes«) des Dienstleistungshandels. Obwohl es zum Zeitpunkt des Inkrafttretens von GATS viele elektronische Dienstleistungen noch nicht gab, deckt die GATS-Klassifizierung zahlreiche digital verfügbare Dienstleistungen mit ab. Einige Dienstleistungen können, müssen aber nicht digital erbracht werden.

79 WTO-Mitgliedstaaten schlossen 1996 das Informationstechnologie-Abkommen (Information Technology Agreement, ITA) ab. Es gewährt Zollfreiheit für bestimmte IT-Produkte wie Computer, Telekommunikationsausrüstung und Halbleiter. ITA gilt jedoch nicht für Dienstleistungen und enthält keine zusätzlichen Aussagen oder Regelungen zum Datenschutz. Es erweitert lediglich die Güterpalette des im Rahmen der WTO liberalisierten Handels mit IT-Produkten und unterliegt vollumfänglich dem Regelwerk der WTO. Nach 17 Verhandlungsrunden der inzwischen 54 Mitgliedstaaten wurde auf der WTO-Ministerkonferenz in Nairobi im Dezember 2015 die Handelsliberalisierung für zusätzlich 201 IT-Produkte beschlossen. Das jährliche Volumen des Handels mit diesen Produkten beläuft sich auf über 1,3 Billionen US-Dollar und macht heute etwa 7% des globalen Handels aus.

Unter Datenschutzaspekten interessant ist vor allem der Handel mit Daten, als Ware oder als Bestandteil von Waren. Die Erbringung digitaler Dienstleistungen ist in der Regel nicht nur mit dem Transfer von Daten verbunden, sondern führt häufig zur Bildung großer Datenmengen (Big Data), die für sich wieder ökonomisch interessant werden. So sammeln beispielsweise Sportuhren millionenfach persönliche Gesundheitsdaten, deren Aggregierung beispielsweise der Pharmaindustrie wichtige Informationen liefert. Fragen des Datenschutzes sind daher in vielen Bereichen des digitalen Dienstleistungshandels in einem Ausmaß berührt, das zur Zeit der Formulierung des Allgemeinen Zoll- und Handelsabkommens (GATT) 1947 und von GATS nicht vorherzusehen war. Heute sind unterschiedliche nationale Regeln zur Datenspeicherung kaum bis gar nicht aufeinander abgestimmt und ihr Zusammenhang mit internationalem Handelsrecht ist nicht eindeutig. Die rechtliche Grundlage für Datenschutzregeln wird durch die in GATT und GATS bestehenden Ausnahmetatbestände geschaffen. Im GATS

- besagt Artikel III, dass das Abkommen nicht zur Preisgabe vertraulicher Informationen verpflichtet, sofern dies unter anderem dem öffentlichen Interesse widerspricht;
- bekräftigt Artikel XIV (als eine allgemeine Ausnahme) das Recht der Mitgliedstaaten, Maßnahmen zu ergreifen, die sicherstellen, dass ihre Gesetze und Regulierungen eingehalten werden. Dies gilt unter anderem für den Schutz der Privatsphäre von Individuen in Bezug auf die Verarbeitung und Verbreitung persönlicher Daten.

Der GATS-Annex zu Finanzdienstleistungen legt in Artikel 2 (Innerstaatliche Vorschriften) fest, dass Mitglieder keine Informationen offenlegen müssen, die sich auf die Geschäfte und Konten von Individuen beziehen oder auf vertrauliche oder sonstige Informationen, die sich im Besitz öffentlicher Stellen befinden.

Bezüge zum Datenschutz im Dienstleistungsabkommen TiSA

Das GATS hat die Grundlagen geschaffen für eine fortzusetzende weitere Liberalisierung des Handels mit Dienstleistungen, die ursprünglich auf multilateraler Ebene stattfinden sollte. Allerdings waren nicht alle Mitgliedstaaten an weiteren Öffnungs-

schritten im Dienstleistungssektor interessiert. Darum werden unter dem Dach der WTO gegenwärtig lediglich plurilaterale Verhandlungen über ein Abkommen zum Handel mit Dienstleistungen (TiSA) geführt. Darüber hinaus verhandelt die EU unter anderem auch über neue internationale Prinzipien für heimische Regulierung, über Informations- und Kommunikationstechnologiedienstleistungen (einschließlich grenzüberschreitenden Datentransfers), elektronischen Handel und computerbezogene Dienstleistungen.

Mit Verweis auf Fragen des Datenschutzes betont die EU-Kommission, dass TiSA die gleichen Schutzmechanismen enthalten wird wie GATS. Zugleich heißt es, dass die in TiSA diskutierten Regeln zum Datentransfer inspiriert seien von ähnlichen Bestimmungen in existierenden Freihandelsabkommen, beispielsweise mit Südkorea. Artikel 7.43 dieses Abkommens hält explizit fest, dass jede Vertragspartei angemessene Regeln zum Schutz der Privatsphäre entwickeln soll, insbesondere mit Blick auf den Transfer persönlicher Daten. Mit dieser Formulierung geht das Südkorea-Abkommen weiter als die bisherigen Ausnahmeregeln. Es sieht die zu vereinbarenden Regeln nicht als mögliche Ausnahme vom freien Handel an, sondern betont die Notwendigkeit, ausreichende Schutzmechanismen *überhaupt zu entwickeln*. Kritiker fürchten allerdings, dass die USA ihre Interessen in den TiSA-Verhandlungen bereits durchgesetzt haben und TiSA freien Datentransfer zwischen den Mitgliedsländern vorsieht.

Bezüge zum Datenschutz in den TTIP-Verhandlungen

Die EU verhandelt derzeit auch in bi- bzw. regionalen Zusammenhängen. So strebt beispielsweise die EU in ihrem Mandat für das transatlantische Freihandelsabkommen TTIP ebenfalls eine Liberalisierung des Dienstleistungssektors an. Es wird erwartet, dass TTIP erhebliche Auswirkungen auf Belange des Datenschutzes haben könnte. Dabei unterscheiden sich die Positionen von EU und USA grundsätzlich, weil die Regelungshistorie, die ökonomische Ausgangssituation und die gesellschaftlichen Präferenzen voneinander abweichen. Angesichts der eingangs erwähnten stark wachsenden Bedeutung von Waren und Dienstleistungen aus dem Informationstechnologie-Sektor haben die USA, aber auch Teile der europäischen Wirtschaft ein großes Interesse an freiem grenzüberschreitendem Datenaustausch. Thilo Weichert vom Datenschutzzentrum Schleswig-Holstein weist darauf hin, dass im Zusammenhang mit »Computerdiensten« praktisch über die Verarbeitung sämtlicher personenbezogener kommerzieller Daten verhandelt wird. Datenschützer hegen große Befürchtungen, dass auch das TTIP Regeln setzen wird, die den Datenschutz in der EU erschweren oder ihm gar zuwiderlaufen könnten.

Nach dem Mandat der EU für TTIP soll für die Europäische Union und ihre Mitgliedstaaten das Recht auf Regulierung bekräftigt werden. Die EU strebt daher an, das explizite Recht der Parteien zu verankern, Maßnahmen zu ergreifen, um legitime innerstaatliche und europäische Politikziele zur Wahrung der nationalen Sicherheit und der inneren Sicherheit der EU zu erreichen. Beim Agendapunkt Dienstleistungen wird Bezug genommen auf die allgemeinen Ausnahmeklauseln des GATS.

Wie schon eingangs gesagt wird im Rahmen des TTIP nicht über Fragen des Datenschutzes verhandelt, die im Folgeabkommen zu Safe Harbor geregelt werden sollen. Prinzipiell geht man ohnehin davon aus, dass die Verankerung der Ausnahmeregeln des GATS in den gegenwärtig verhandelten Freihandelsabkommen ausreichenden Schutz bietet und Politikspielraum gewährt.

Datenschutzentwicklung in Europa

Nachdem die OECD im Jahr 1980 erstmals rechtsunverbindliche Datenschutzbestimmungen (Privacy Guidelines) beschlossen hatte, wurde im Europarat 1981 die erste rechtsverbindliche Datenschutzkonvention verabschiedet. Die 1995 von den EU-Mit-

gliedstaaten beschlossene und noch immer geltende Datenschutzrichtlinie verfolgt zwei gleichberechtigte Ziele: den »Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten« und den »freien Datenverkehr«. 2002 folgte die Datenschutzrichtlinie für elektronische Kommunikation (ePrivacy-Richtlinie). Die ergänzende Cookie-Richtlinie aus dem Jahr 2009 trifft Regelungen für den Schutz personenbezogener Daten, die bei der individuellen Internetnutzung in Form entsprechender Cookies generiert werden.

Nach den Enthüllungen von Edward Snowden ging der Facebook-Kritiker Maximilian Schrems im Juni 2013 mit einer Beschwerde gegen Facebook Irland vor. Es folgten die richtungsweisenden EuGH-Urteile zur Vorratsdatenspeicherung vom April 2014 und zum »Recht auf Vergessenwerden« vom Mai 2014. Damit wurde eine Überprüfung aller EU-Bestimmungen in Gang gesetzt, die den Schutz und die Sicherheit von Daten betreffen. Weitere Anforderungen ergeben sich durch das Safe-Harbor-Urteil des EuGH vom Oktober 2015. Nicht zuletzt haben sich Mitte Dezember 2015 das Europäische Parlament (EP), der Ministerrat und die Kommission auf eine neue Datenschutz-Grundverordnung (DS-GVO) geeinigt. Der Innen- und Justizausschuss des Europäischen Parlaments (EP) hat diese Verordnung mit großer Mehrheit angenommen: 48 Ja-Stimmen standen nur 4 Nein-Stimmen und 4 Enthaltungen gegenüber. Ministerrat und das EP-Plenum müssen noch zustimmen. Anfang 2018 wird damit die erste umfassende Rechtsnorm zur Reform des seit 1995 geltenden EU-Datenschutzrechts in Kraft treten und unmittelbar in nationales Recht umzusetzen sein. Die Verordnung gilt für den gesamten privaten und öffentlichen Bereich. Ausgenommen sind lediglich Polizei und Justiz, für die gleichzeitig eine neue Datenschutzrichtlinie verhandelt wurde.

Die Datenschutz-Grundverordnung

Mit der DS-GVO wird es erstmals ein einheitliches verbindliches Schutzniveau für die gesamte EU geben. Auf diese Weise soll ein Wettbewerb um die Bestimmungen mit dem geringsten Schutz in der EU vermieden werden. »Europäisches Recht auf europäischen Boden«, so lautet das Leitmotiv der Kommission. Die Neuregelung sieht vor, dass Internetkonzerne in Zukunft die ausdrückliche Zustimmung der Nutzer einholen müssen, wenn sie deren Daten verwenden wollen. Nutzer erhalten zudem das Recht, gespeicherte Informationen wieder löschen zu lassen (»Recht auf Vergessenwerden«) und Daten eines Anbieters bei einem Wechsel zum nächsten mitzunehmen (»Portabilität«). Unternehmen müssen ihre Produkte datenschutzfreundlich voreinstellen (Privacy by Design und by Default). Neue Anforderungen an den Schutz und die Sicherheit von Daten sollen IT-Produkte fördern, deren technologische Ausgestaltung den Schutz privater Daten erleichtert.

An die neuen Regeln müssen sich nicht nur europäische Unternehmen halten, sondern auch Firmen aus Drittstaaten. Wenn anbietende Unternehmen gegen sie verstoßen, drohen ihnen hohe Strafen von bis zu vier Prozent ihres weltweiten Jahresumsatzes. Hat ein Verbraucher ein Problem mit dem Anbieter in einem anderen EU-Land, soll er sich künftig in seiner Sprache an die heimische Beschwerdestelle wenden können.

Datenschutzbehörden nehmen als Beschwerde- und Kontrollstelle eine zusehends wichtigere Funktion wahr. Denn sie achten darauf, wie mit personenbezogenen Daten in der Informationsgesellschaft umgegangen wird, und sie können Sanktionen veranlassen. Der EuGH hat in zwei Urteilen (2010, 2012) die Notwendigkeit der »völligen Unabhängigkeit« von Datenschutzbeauftragten und ihren Behörden betont, um eine Einflussnahme Dritter zu begrenzen.

Einige Punkte der DS-GVO werden durchaus kritisch gesehen. In der EU ist die Datenverarbeitung jeweils an einen Zweck gebunden. Der Zweck begründet die Daten-

verwendung. Die USA hingegen kennen das Erforderlichkeits- und Zweckbindungsprinzip nicht. Die vorgesehene Zweckbindung widerspricht der Geschäftslogik der aufstrebenden Ökonomie von Plattformen wie Alibaba oder ebay fundamental. Im Fall von Big Data wird das Konzept der Zweckbindung systematisch untergraben, da es bei dem Anhäufen und Analysieren riesiger Datenmengen genau darum geht, Daten nicht nur viele Male für denselben Zweck zu nutzen, sondern auch für viele unterschiedliche Zwecke. Dabei sind es häufig erst Big-Data-Analysen, die vor allem aufgrund statistischer Zusammenhänge neue Möglichkeiten zur Nutzung personenbezogener Daten entstehen lassen.

Der in der DS-GVO gefundene Kompromiss sieht Ausnahmen für die Wissenschaft vor, so dass pseudonymisierte Daten auch zu kommerziellen Forschungszwecken verwendet werden dürfen. Beispielsweise ist die Nutzung von Verwaltungsdaten relevant für weite Teile der Arbeitsmarktforschung. Nach der Neuregelung müssen bei jeder Untersuchung eindeutige Indizien für eine Einwilligung vorliegen. An enge Kriterien gebundene Einwilligungserklärungen beeinträchtigen aber die empirische Forschung, die aufgrund geringer Teilnahmebereitschaft ohnehin schon erschwert ist.

Kritisch gesehen werden auch die Möglichkeiten der US-amerikanischen Sicherheitsbehörden und europäischen Geheimdienste, in Belangen, die die nationale Sicherheit betreffen, auf Daten zuzugreifen, die in den verschiedensten EU-Staaten nach unterschiedlichen Geheimdienstrechten gespeichert und verfügbar sind. Diese Möglichkeiten bleiben erhalten und werden auch in Zukunft im Widerspruch zum einheitlichen EU-Datenschutzrecht stehen. Zum Reformpaket der DS-GVO gehört zwar auch die Richtlinie für einen harmonisierten Rechtsrahmen zur Datenverarbeitung von Polizei- und Justizbehörden in EU-Ländern. Eine verbindliche transatlantische Verständigung über die Zusammenarbeit zwischen den Geheimdiensten gehört aber nicht dazu.

Das Safe-Harbor-Abkommen und »EU-US Privacy Shield«

Für den weltweit größten Wirtschaftsraum, der die USA und die EU umfasst, wurde im Jahr 2000 das sogenannte Safe-Harbor-Abkommen beschlossen. Es soll sicherstellen, dass US-Unternehmen die Daten europäischer Nutzer angemessen schützen, wenn die Unternehmen diese Daten in den USA weiterverarbeiten. Faktisch, aber nicht de jure handelte es sich um eine Entscheidung der Kommission. Darin hat sie Unternehmen als sicheren Hafen eingestuft, die sich zur Einhaltung bestimmter Datenschutzstandards verpflichtet und der Kontrolle durch die US-amerikanische Handelsaufsichtsbehörde (Federal Trade Commission, FTC) unterworfen haben. Die FTC-Vertreterin, Julie Brill, verwies darauf, dass es in den 15 Jahren des Bestehens von Safe Harbor gerade einmal vier Hinweise europäischer Datenschutzbehörden auf Verstöße gegeben habe. Insgesamt haben 4400 Unternehmen Daten auf Basis des Abkommens in die USA übertragen. Die FTC sei in diesem Zeitraum zahlreichen Verstößen nachgegangen und habe in 39 Fällen rechtliche Schritte gegen Unternehmen eingeleitet – darunter auch Facebook. Die niedrige Zahl rechtlich relevanter Fälle könnte ein Hinweis auf die geringe Wirksamkeit von Safe Harbor sein.

Der EuGH hat im Oktober 2015 diese Regelung zum wirtschaftlichen Austausch von Daten zwischen den USA und der EU für ungültig erklärt. Er folgte damit einer Klage, die der österreichische Jurist Maximilian Schrems angestrengt hatte. Der EuGH berief sich in seinem Urteil auf den Vertrag von Lissabon und die Charta der Grundrechte der EU, die der »Achtung des Privat- und Familienlebens« und dem »Schutz personenbezogener Daten« den Status eines Grundrechts verliehen haben. Der EuGH hat insbesondere den Zugriff von US-Behörden auf die Daten europäischer Nutzer kritisiert.

Die EU-Datenschutzbehörden hatten der EU-Kommission bis Ende Januar Zeit gegeben, um mit den USA über ein neues Abkommen zu verhandeln. Anfang Februar

2016 haben sich EU und USA auf eine neue Regelung zum künftigen Datenaustausch zwischen den Wirtschaftsräumen geeinigt, den »EU-US Privacy Shield«. Das US-Handelsministerium soll danach jene Firmen kontrollieren, die Daten aus Europa verarbeiten. Wer sich nicht an die Standards hält, soll von der Liste der Unternehmen, die Daten verarbeiten dürfen, gestrichen werden oder Strafgebühren zahlen. Die US-Seite stimmte einer Aufsicht durch die eigenen Justiz- und Sicherheitsbehörden zu. Alljährlich sollen beide Partner die Umsetzung des Abkommens überprüfen. Wer seine Datenschutzrechte verletzt sieht und die Verletzung unter Berufung auf die nationale Sicherheit der USA erfolgt, soll sich an einen Ombudsmann wenden dürfen, der unabhängig von den US-Sicherheitsbehörden arbeiten soll. Das EU-Recht verlangt hier eine Rechtsgarantie. In Konfliktfällen soll es ein kostenloses Schlichtungsverfahren geben.

Ein weiteres Problem stellt die Vorratsdatenspeicherung dar. Die USA weisen darauf hin, dass die Neuregelungen des USA Freedom Act die anlasslose Vorratsdatenspeicherung nur zulassen, wenn sie strafrechtlich relevanten Zwecken dient. Die US-Regelungen betreffen allerdings nur Ermittlungen in Amerika, die sich gegen Amerikaner richten. Die Kommission setzt darauf, dass die USA EU-Bürgern direkten Zugang zu amerikanischen Gerichten gewähren, um dort gegen den möglichen Missbrauch ihrer Daten vorgehen zu können. Das Abkommen setzt voraus, dass die europäischen Datenschutzbehörden und die zuständigen amerikanischen Behörden, allen voran die Aufsichtsbehörde FTC, eng zusammenarbeiten. Sobald die Kommission die rechtlichen Grundlagen transparent gemacht hat, können EU-Datenschützer Privacy Shield vor dem Hintergrund der EuGH-Anforderungen prüfen und die EU-Staaten über das Abkommen abstimmen.

Die Rechtsunsicherheit wird mittelfristig anhalten. Der EuGH hatte sehr enge Vorgaben für eine widerspruchsfreie Umsetzung von EU-US-Privacy Shield gemacht. Viele teilen die Rechtsauffassung der Juristin Emma Peters von der Humboldt-Universität, dass der EuGH mit dem Schrems-Urteil zu weit vorgeprescht sei. Demnach verlange der EuGH »von den USA einen Schutzstandard für die Daten der Unionsbürger, den er von seinen eigenen Mitgliedsstaaten nicht verlangen kann – und die diese den US-Bürgern nach derzeitigem Kenntnisstand auch ihrerseits nicht zukommen lassen« (JUWiss-Blog, 14.10.2015).

Schlussfolgerungen

Der europäische Datenschutz wird den künftigen transatlantischen Datentransfer stark beeinflussen. TTIP mag in getrennten Runden ausgehandelt werden, steht aber inhaltlich und fachlich in einem direkten Zusammenhang mit den diversen Datenschutzreformen der EU. Ob die parallelen Verhandlungsstränge miteinander vereinbar sind, ist strittig. Insofern ist es von zentraler Bedeutung, dass TTIP und TiSA ausreichende Flexibilität lassen, um noch zu definierende EU-Regeln für den Datenschutz auch in den künftigen europäischen Handelsbeziehungen berücksichtigen zu können. Datenschützer fordern deshalb, dass durch TTIP keine Festlegungen getroffen werden dürfen, die die Umsetzung einer EU-DS-GVO beeinträchtigen. Alle Unklarheiten würden Unternehmen Möglichkeiten eröffnen, später Klagen zu erheben, wenn sie den Eindruck gewinnen, die EU-Regelungen stünden im Widerspruch zu den getroffenen internationalen Vereinbarungen. Im Falle des TTIP könnten solche Klagen im Rahmen von Investor-Staats-Verfahren erhoben werden, was die Befürchtungen von Kritikern zusätzlich befeuert. Ob es gelingen kann, trotz TTIP und TiSA für ausreichend Flexibilität zu sorgen, um die EU-Datenschutzregeln wirksam umzusetzen, hängt vor allem von folgenden Faktoren ab:

- Da die DS-GVO vor TTIP und TiSA abgeschlossen wurde, ist es noch möglich, die Abkommenstexte und die datenschutztechnischen Implikationen der Liberalisierungszugeständnisse zu überprüfen.

- Ebenfalls zu prüfen gilt, ob die Ausnahmebestimmungen des GATS bzw. die noch zu definierenden von TTIP und TiSA ausreichend schlagkräftig und eindeutig formuliert sind.
- Bedeutsam ist auch die Frage, inwieweit (handelspolitische) Fachleute die technischen und datenschutzrelevanten Folgen von Liberalisierungsvereinbarungen für Dienstleistungen richtig abschätzen können, die erst in der Zukunft entwickelt werden. Diese Frage ist insbesondere bei Festlegungen im Kontext des sogenannten Negativlisten-Ansatzes von Verhandlungen relevant. Im Sinne dieses Ansatzes wird ein Sektor in Gänze liberalisiert, mit Ausnahme solcher Aktivitäten, die speziell aufgeführt werden. Dieser Ansatz birgt die große Gefahr, dass die Liberalisierung Produkte mit hoher Datenschutzrelevanz umfasst, die erst noch entwickelt werden und bei denen man die datenschutzrechtlichen Folgen der Liberalisierung noch nicht abschätzen kann.
- Wichtig sind nicht zuletzt eine klare Definition neuer digitaler Dienstleistungen und die Klärung der Frage, inwieweit sie eindeutig einer der vier WTO-Erbringungsarten (siehe oben, S. 3) zuzuordnen sind.

In dieser Situation empfiehlt es sich, eine Formulierung in neu zu verhandelnde Freihandelsabkommen aufzunehmen, die zumindest den Klauseln im Südkorea-Abkommen entspricht; denn diese sind eindeutiger als die Ausnahmeklauseln des GATS.

All diese Faktoren legen nahe, dass künftig die Akteure aus den Bereichen Informations- und Kommunikationstechnologie, Datenschutz und Handelsverhandlungen enger kooperieren.

Die neue EU-Handelsstrategie »Trade for all« von Oktober 2015 bietet erste Ansatzpunkte für die weiterhin notwendige Diskussion über das Verhältnis von Handel und Datenschutz. Unternehmen streben zwar möglichst freie Datenflüsse an, sind aber gleichzeitig auf die Sicherheit ihrer Daten (und insbesondere auf den Schutz geistigen Eigentums) angewiesen. Das Thema Datensicherheit wird in der im Dezember 2015 verabschiedeten EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS) aufgegriffen. Sie sieht eine Pflicht zur Meldung schwerwiegender Cyberattacken sowie Mindestanforderungen an die Sicherheit der Daten vor, die mit dem Schutz kritische Infrastruktur verbunden sind. Das vergleichbare Gesetz in den USA, der Cybersecurity Information Sharing Act (CISA), ist weniger weitreichend. Danach dürfen US-Unternehmen bei nicht näher spezifizierten IT-Bedrohungen Daten an US-Behörden wie das Heimatschutzministerium weitergeben, die sie wiederum anderen Institutionen wie FBI und NSA zuleiten können. Kritiker stören sich daran, dass dem Datenschutz nicht ausreichend Rechnung getragen wird. Aus Sicht multinationaler Unternehmen wäre eine möglichst einheitliche Regelung auf beiden Seiten des Atlantiks wünschenswert.

Insgesamt herrscht in der derzeitigen Situation Rechtsunsicherheit bei Unternehmen und Verbrauchern im transatlantischen Wirtschaftsraum. Lösungen liegen nicht unmittelbar auf der Hand. Die IT-Industrie richtet sich bereits auf striktere Regelungen ein, indem sie pseudonymisierte Lösungen, Verschlüsselungen und andere Verfahren der Anonymisierung von personengebundenen und Metadaten anwenden. US-Firmen wie Microsoft haben unmittelbar auf das Safe-Harbor-Urteil reagiert und wollen den Kunden ihrer Cloud-Dienste künftig die Speicherung und Verarbeitung ihrer Daten in Deutschland ermöglichen. Dafür sollen Rechenzentren der deutschen Telekom genutzt werden. Als Treuhänderin soll die Telekom-Tochter T-Systems den internationalen Zugang zu den Kundendaten kontrollieren und überwachen. Microsoft und seine Auftragnehmer hätten infolgedessen nur noch Zugriff auf die Daten, wenn T-Systems oder die Endkunden einwilligen. Ein gangbarer Weg auch für andere Cloud-Dienste ist demnach die Schaffung einer Serverinfrastruktur innerhalb der EU bei gleichzeitiger rechtlicher und technischer Ausgliederung von Zugriffsrechten.

SWP
Stiftung Wissenschaft und Politik
Deutsches Institut für Internationale Politik und Sicherheit

Ludwigkirchplatz 3–4
10719 Berlin
Telefon +49 30 880 07-0
Fax +49 30 880 07-100
www.swp-berlin.org
swp@swp-berlin.org

ISSN 1611-6364